6.4 Proof by Cases and Disproofs

In the last proof of the previous section, we did something interesting: having concluded that $d_1 < 2$ or $d_1 > \sqrt{p}$, we proceeded to split up our proof into two cases, one where we assumed that each part of the OR was true. This is a proof technique known as **proof by cases**.

Proof by cases

Remember that for a universal proof, we typically let a variable be an arbitrary element of the domain, and then make an argument in the proof body to prove our goal statement. However, even when the goal statement is True for all elements of the domain, it isn't always easy to construct a single argument that works for all of those elements! Sometimes, different arguments are required for different elements. In this case, we divide the domain into different parts, and then write a separate argument for each part.

A bit more formally, we pick a set of unary predicates P_1, P_2, ..., P_k (for some positive integer k), such that for every element x in the domain, x satisfies at least one of the predicates (we say that these predicates are *exhaustive*). Note that the domain can be narrowed based on additional assumptions or conclusions made earlier in the proof. In our previous example, we started with a domain "$d_1 \in \mathbb{N}$", and then narrowed this to "$d_1 \in \mathbb{N}$ and $(d_1 < 2 \lor d_1 > \sqrt{p})$", leading to the following predicates for our cases:

$$P_1(d_1) : d_1 < 2, \qquad P_2(d_1) : d_1 > \sqrt{p}.$$

Then, we divide the proof body into cases, where in each case we *assume* that one of the predicates is True, and use that assumption to construct a proof that specifically works under that assumption.[1]

A typical proof by cases.

Given statement to prove: $\forall x \in S, P(x)$. Pick a set of exhaustive predicates $P_1, \ldots, P_k$ of S.

Proof. Let $x \in S$. We will use a proof by cases.

Case 1. *Assume* $P_1(x)$ is True.

[Proof that $P(x)$ is True, assuming $P_1(x)$.]

Case 2. *Assume* $P_2(x)$ is True.

[1] Recall that there's an equivalence between predicates and sets. Another way of looking at a proof by cases is that we divide the domain into subsets $S_1, S_2, \ldots S_k$, and then prove the desired statement separately for each of these subsets.

[Proof that $P(x)$ is True, assuming $P_2(x)$.]

$\vdots$

Case k. *Assume* $P_k(x)$ is True.

[Proof that $P(x)$ is True, assuming $P_k(x)$.] ■

Proof by cases is a very versatile proof technique, since it allows the combining of simpler proofs together to form a whole proof. Often it is easier to prove a property about some (or even most) elements of the domain than it is to prove that same property about all the elements. But do keep in mind that if you can find a *simple* proof which works for all elements of the domain, that's generally preferable than combining multiple proofs together in a proof by cases.

Cases and the Quotient-Remainder Theorem

One natural use of proof by cases in number theory is to apply the Quotient-Remainder Theorem that we introduced in Section 6.1.

Theorem. (Quotient-Remainder Theorem) For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ such that $n = qd + r$ and $0 \leq r < d$. Moreover, these q and r are *unique* for a given n and d.

We say that q is the **quotient** when n is divided by d, and that r is the **remainder** when n is divided by d.

The reason this theorem is powerful is that it tells us that for any non-zero divisor $d \in \mathbb{Z}^+$, we can separate all possible integers into d different groups, corresponding to their possible remainders (between 0 and $d - 1$) when divided by d. Let's see this how to use this fact to perform a proof by cases.

Example. Prove that for all integers x, $2 \mid x^2 + 3x$.

Translation. Using the divisibility predicate: $\forall x \in \mathbb{Z},\ 2 \mid x^2 + 3x$. Or expanding the definition of divisibility:

$$\forall x \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ x^2 + 3x = 2k.$$

Discussion. We want to "factor out a 2" from the expression $x^2 + 3x$, but this only works if x is even. If x is odd, though, then both x^2 and $3x$ will be odd, and adding two odd numbers together produces an even number.

But how do we "know" that every number has to be either even or odd? And how can we formalize the algebraic operations of "factoring out a 2" or "adding two odd numbers together"? This is where the Quotient-Remainder Theorem comes in.

Proof. Let $x \in \mathbb{Z}$. By the Quotient-Remainder Theorem, we know that when x is divided by 2, the two possible remainders are 0 and 1. We will divide up the proof into two cases based on these remainders.

Case 1: assume the remainder when x is divided by 2 is 0. That is, we assume there exists $q \in \mathbb{Z}$ such that $x = 2q + 0$. We will show that there exists $k \in \mathbb{Z}$ such that $x^2 + 3x = 2k$.

We have:

$$\begin{aligned} x^2 + 3x &= (2q)^2 + 3(2q) \\ &= 4q^2 + 6q \\ &= 2(2q^2 + 3q) \end{aligned}$$

So let $k = 2q^2 + 3q$. Then $x^2 + 3x = 2k$.

Case 2: assume the remainder when x is divided by 2 is 1. That is, we assume there exists $q \in \mathbb{Z}$ such that $x = 2q + 1$. We will show that there exists $k \in \mathbb{Z}$ such that $x^2 + 3x = 2k$.

We have:

$$\begin{aligned} x^2 + 3x &= (2q+1)^2 + 3(2q+1) \\ &= 4q^2 + 4q + 1 + 6q + 3 \\ &= 2(2q^2 + 5q + 2) \end{aligned}$$

So let $k = 2q^2 + 5q + 2$. Then $x^2 + 3x = 2k$. ■

False statements and disproofs

Suppose we have a friend who is trying to convince us that a certain statement X is False. If they tell you that statement X is false because they tried really hard to come up with a proof of it and failed, you might believe them, or you might wonder if maybe they just missed a crucial idea leading to a correct proof.[2] An absence of proof is not enough to convince us that the statement is False.

Instead, we must see a **disproof**, which is simply a proof that the *negation* of the statement is True.[3] For this section, we'll be using the simplification rules from Section 3.2 to make negations of statements easier to work with.

Example. Disprove the following statement: every natural number divides 360.

Translation. This statement can be written as $\forall n \in \mathbb{N},\ n \mid 360$. However, we want to prove that it is False, so we really need to study its negation.

$$\begin{aligned} &\neg\big(\forall n \in \mathbb{N},\ n \mid 360\big) \\ &\quad \exists n \in \mathbb{N},\ n \nmid 360 \end{aligned}$$

Discussion. The original statement is obviously not True: the number 7 doesn't divide 360, for instance. Is that a proof? We wrote the negation of the statement in symbolic form above, and if we translate it back into English, we get "there exists a natural number which does not divide 360." So, yes. That's enough for a proof.

Proof. Let $n = 7$.

Then $n \nmid 360$, since $\frac{360}{7} = 51.428\ldots$ is not an integer. ■

When we want disprove a universally-quantified statement ("every element of S satisfies predicate P"), the negation of that statement becomes an existentially-quantified one ("there exists an element of S that doesn't satisfy predicate P"). Since proofs of existential quantification involve just finding one value, the disproof of the original statement involves finding such a value which causes the predicate to be False (or alternatively, causes the negation of the predicate to be True). We call this value a **counterexample** for the original statement. In the previous example, we would say that 7 is a counterexample of the given statement.

A typical disproof of a universal (counterexample).

[2] Maybe they skipped all their CSC110 classes.

[3] In other words, if we can prove that $\neg X$ is True, then X must be False.

Given statement to *disprove*: $\forall x \in S,\ P(x)$.

Proof. We prove the negation, $\exists x \in S,\ \neg P(x)$. Let $x =$ _______.

[Proof that $\neg P($_______$)$ is True.] ■